UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/792,236	03/03/2004	Michael Thomas Kurdziel	RF-234 (50588)	4669

74701 7590 03/12/2009

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST
255 S ORANGE AVENUE
SUITE 1401
ORLANDO, FL 32801

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
03/12/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Office Action Summary	Application No.	Applicant(s)	
	10/792,236	KURDZIEL, MICHAEL THOMAS	
	Examiner	Art Unit	
	Christian LaForgia	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The Applicant's response of 09 December 2008 has been noted and made of record.

2. Claims 1-38 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-38 have been considered but are moot in view of the new grounds of rejection set forth below.

Terminal Disclaimer

4. The terminal disclaimer filed on 09 December 2008 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of U.S. Patent No. 6,108,421 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,108,421 to Kurdziel et al., hereinafter Kurdziel, in view of U.S. Patent No. 5,623,549 to Ritter, hereinafter Ritter.

7. As per claims 1 and 13, Kurdziel teaches a block cipher device and a communication system for a cryptographically secured digital communication system comprising:

a pair of first stages receiving an input data block and a control data block (claim 1(a) a first stage to receive an input data block and control data block), each first stage defining a respective first data path and comprising

a sum modulo-two unit responsive to the control data block and the input data block (claim 1(a)(i) a sum modulo-two unit responsive to the input data block and a first subset of the control data block), and

a first nibble swap unit downstream from said sum modulo-two unit and being responsive to an output signal therefrom and the control data block for reordering the output signal from said sum modulo-two unit (claim 1(a)(ii) a first nibble swap unit responsive to the output signal from said sum modulo-two unit and a second subset of the control data block for reordering the output signal from said sum modulo-two unit);

a key scheduler receiving a key data block and generating a random key data block based thereon (claim 1(b) a key scheduler responsive to a key data block including means for randomizing the key data block);

a pair of second stages connected in parallel (column 2, line 13, i.e. serial and parallel are interchangeable based on the intended use) downstream from said first stages and receiving the random key data block, the control data block and output signals from said first stages, each second stage defining a respective second data path (claim 1(c) a second stage adapted to receive the randomized key data block from said key scheduler in first and second key data sub-blocks, the control data block and the output signal from said first stage) and comprising

a first linear modulo unit responsive to the random key data block, one of the output signals from said first stages, and the control data block for performing a modulo summing operation based on a first modulus q (claim 1(c)(i) a first linear modulo unit responsive to said first key data sub-block from the key scheduler, the output signal from said first stage, and the control data block for performing a modulo summing operation based on a first modulo q),

an n^{th} power modulo unit responsive to an output signal from said first linear modulo unit for performing an n^{th} power modulo operation based on a second modulus p (claim 1 (c)(ii) an n^{th} power modulo unit responsive to the output signal from said first linear modulo unit for performing an n^{th} power modulo operation based on a second modulus p), and

a second linear modulo unit responsive to the random key data block and an output signal from said n^{th} power modulo unit for performing a modulo summing operation based on a third modulus r (claim 1(c)(iii) a second linear modulo unit responsive to the second key data sub-block and output from said n^{th} power modulo unit for performing a modulo summing operation based on a third modulus r),

each first, second and third modulus q, p and r being unique from each other (claim 1 said first, second, and third modulus p, q, and r respectively being unique from each other); and

an output stage connected to said second stages for generating an output data block for the block cipher device (Figure 4 [element 11], column 2, lines 9-14).

8. Kurdziel does not teach wherein the first stages are connected in parallel and a diffuser connected in both of the first data paths for mixing data therebetween.

9. Ritter discloses the first stages of a block cipher connected in parallel (Figures 5(a) [elements 156a, 156b], 5(b) [elements 158a, 158b], column 8, line 53 to column 9, line 13) and a device to mix the information on both data paths (Figures 5(a) [element 152], 5(b) [element 154], column 8, line 53 to column 9, line 13, column 10, line 57 to column 11, line 50) .

10. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Kurdziel such that wherein the first stages were connected in parallel and to include a diffuser connected in both of the first data paths for mixing data therebetween, since

Ritter states at column 5, line 60 to column 6, line 9 that including block mixers enhances cryptographic mechanisms by increasing the size of the blocks, thereby making the encrypted data more difficult to crack. The block mixers further enhance security by having every possible input block produce a different output block, and every possible output block is produced by a different input block; each output block being a function of both input blocks; any change to any one of the input block values changes both of the output block values; and stepping either of the input blocks through all possible values while keeping the other of the input blocks fixed steps each of the output blocks through all possible values (Ritter; column 6, lines 10-25).

11. Regarding claims 2 and 18, Kurdziel teaches wherein said first and second stages are selectively configurable so that one first data path and one second data path are operational (Figure 4, column 2, line 10-15).

12. As noted above, Kurdziel does not disclose a diffuser, nor that it would be bypassed.

13. It would have been obvious to one of ordinary skill in the art at the time the invention was made since it has been held that it only requires routine skill in the art to eliminate an element and its function. See MPEP 2144.04; see *Ex parte Wu*, 10 USPQ 2031 (Bd. Pat. App. & Inter. 1989). This is further supported by the fact that Kurdziel discloses a similar system that functions without the diffuser mixing bits.

14. Regarding claims 3 and 19, Ritter teaches wherein said diffuser is connected in both of the first data paths between the respective sum modulo-two units and first nibble swap units (Figures 5(a) [element 152], 5(b) [element 154], column 8, line 53 to column 9, line 13, column

10, line 57 to column 11, line 50).

15. Regarding claims 4 and 20, Kurdziel teaches wherein each first stage further comprises a substitution/expansion unit downstream from said first nibble swap unit and being responsive to an output signal therefrom for providing customizable cipher variations (claim 2).

16. With regards to claims 5 and 21, Kurdziel teaches a second nibble swap unit downstream from said substitution/expansion unit and being responsive to an output signal therefrom and the control data block for reordering the output signal from said substitution/expansion unit (claim 3).

17. Regarding claims 6 and 22, Kurdziel teaches a nibble interleave unit connected in both of the first data paths for reordering data therebetween (Figure 4 [element 4], column 3, lines 5-17, i.e. re-ordering of W_3).

18. Regarding claims 7 and 23, Kurdziel teaches a substitution unit connected in both of the first data paths for substituting data therebetween (Figure 4 [element 3], column 2, line 62 to column 3, line 4).

19. Regarding claims 8 and 24, Kurdziel teaches wherein each n^{th} power modulo unit provides an output signal of predetermined size, with $n>1$ and with $p=2^K-X$, where X is selected such that a greatest common denominator between n and (2^K-X-1) is 1 and K is the

predetermined size (claim 1(c)(ii)).

20. Regarding claims 9 and 25, Kurdziel teaches wherein said key scheduler comprises a pair of look-up tables for generating the random key data block (claim 5).

21. With regards to claims 10 and 26, Kurdziel teaches wherein said key scheduler further comprises a pair of shift registers responsive to the received key data block (claim 6); and wherein each look-up table is responsive to a corresponding shift register (claim 7).

22. Concerning claims 11 and 27, Kurdziel teaches wherein said key scheduler further comprises a pair of combiners responsive to outputs from said shift registers and to outputs from said look-up tables, each combiner combining the output from a corresponding shift register and the output from a corresponding look-up table using a modulo-two summing operation, and each combiner providing a combined data output (claim 8).

23. Regarding claims 12 and 28, Kurdziel teaches wherein each second stage further comprises a non-invertible operation unit downstream from said n^{th} power modulo unit and being responsive to an output signal therefrom, said non-invertible operation unit discarding a portion of the output signal from said n^{th} power modulo unit (claim 13).

24. Regarding claim 14, Kurdziel teaches wherein said first unit comprises a sum modulo-two unit, said second unit comprises a nibble swap unit, and said first and second modulo units

comprise first and second linear modulo units for performing summing operations (claim 11).

25. Regarding claim 15, Kurdziel teaches wherein said block cipher device operates as an encrypter (column 1, lines 30-33).

26. Regarding claim 16, Kurdziel teaches wherein said block cipher device operates as a decrypter (column 1, lines 30-33).

27. Regarding claim 17, Kurdziel teaches further comprising circuitry connected to said block cipher device so that said block cipher device operates in at least one of a block cipher feedback mode, a minimum error propagation mode and a self-synchronizing feedback mode (column 4, lines 38-41).

28. As per claim 29, Kurdziel teaches a method for converting an input data block into an output data block for a cryptographically secured digital communication system, the method comprising:

providing the input data block, a control data block and a random key data block to data paths in the digital communication system (claim 15(a) providing an initial data block, a control data block, a first key data block and a second key data block);

combining the control data block and the input data block within each data path to provide a first data output signal for each data path (claim 15(b) combining the initial data block and the control data block to provide a first data output signal);

transposing segments of the first data output signal within each data path in response to the control data block to provide a second data output signal within each data path (claim 15(c) transposing segments of the first data output signal responsively to a first subset of the control data block to provide a second data output signal);

performing a first linear modulo operation based on a modulus q within each data path in response to the second data output signal, the random key data block and the control data block to provide a third data output signal within each data path (claim 1(c)(i) a first linear modulo unit responsive to said first key data sub-block from the key scheduler, the output signal from said first stage, and the control data block for performing a modulo summing operation based on a first modulo q);

performing an n^{th} power modulo operation based on a second modulus p within each respective data path in response to the third data output signal to provide a fourth data output signal within each data path (claims 1 (c)(ii), 15(g) an n^{th} power modulo unit responsive to the output signal from said first linear modulo unit for performing an n^{th} power modulo operation based on a second modulus p); and

performing a second linear modulo operation based on a third modulus r within each respective data path in response to the random key data block (claim 1(c)(iii) a second linear modulo unit responsive to the second key data sub-block and output from said n^{th} power modulo unit for performing a modulo summing operation based on a third modulus r) and the fourth data output signal to provide an output data block (Figure 4 [element 11], column 2, lines 9-14),

each first, second and third modulus q, p and r being unique from each other (claim 1 said first, second, and third modulus p, q, and r respectively being unique from each other).

29. Kurdziel does not teach wherein the first stages are connected in parallel and a diffuser connected in both of the first data paths for mixing data therebetween.

30. Ritter discloses the first stages of a block cipher connected in parallel (Figures 5(a) [elements 156a, 156b], 5(b) [elements 158a, 158b], column 8, line 53 to column 9, line 13) and a device to mix the information on both data paths (Figures 5(a) [element 152], 5(b) [element 154], column 8, line 53 to column 9, line 13, column 10, line 57 to column 11, line 50) .

31. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Kurdziel such that wherein the first stages were connected in parallel and to include a diffuser connected in both of the first data paths for mixing data therebetween, since Ritter states at column 5, line 60 to column 6, line 9 that including block mixers enhances cryptographic mechanisms by increasing the size of the blocks, thereby making the encrypted data more difficult to crack. The block mixers further enhance security by having every possible input block produce a different output block, and every possible output block is produced by a different input block; each output block being a function of both input blocks; any change to any one of the input block values changes both of the output block values; and stepping either of the input blocks through all possible values while keeping the other of the input blocks fixed steps each of the output blocks through all possible values (Ritter; column 6, lines 10-25).

32. Regarding claim 30, Kurdziel teaches wherein the cryptographically secured digital communication system is selectively configurable so that one data path is operational (Figure 4, column 2, line 10-15).

33. Regarding claim 31, Kurdziel teaches performing a substitution/expansion operation within each data path on the second data output signal to provide customizable cipher variations (claim 2).

34. With regards to claim 32, Kurdziel teaches performing a nibble swap operation within each data path on the customizable cipher variations in response to the control data block for reordering the customizable cipher variations (claim 3).

35. Concerning claim 33, Kurdziel teaches performing a nibble interleave operation for reordering data between the data paths for the reordered customizable cipher variations (Figure 4 [element 4], column 3, lines 5-17, i.e. re-ordering of W_3).

36. Concerning claim 34, Kurdziel teaches performing a substitution operation after the nibble interleave operation for substituting the reordered customizable cipher variations between the parallel data paths (Figure 4 [element 3], column 2, line 62 to column 3, line 4).

37. Regarding claim 35, Kurdziel teaches wherein each n^{th} power modulo unit provides an output signal of predetermined size, with n>1 and with $p=2^K-X$, where X is selected such that a greatest common denominator between n and (2^K-X-1) is 1 and K is the predetermined size (claim 1(c)(ii)).

38. Regarding claim 36, Kurdziel teaches wherein the random key data block is generated by

a key scheduler comprising a pair of look-up tables (claim 5).

39. With regards to claim 37, Kurdziel teaches wherein the key scheduler further comprises a respective shift register associated with each look-up table (claims 6 and 7).

40. Concerning claim 38, Kurdziel teaches wherein the key scheduler further comprises a pair of combiners responsive to outputs from the shift registers and to outputs from the look-up tables, each combiner combining the output from a corresponding shift register and the output from a corresponding look-up table using a modulo-two summing operation, and each combiner providing a combined data output (claim 8).

Conclusion

41. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

42. The following patents are cited to further show the state of the art with respect to a patent related to the inventor of the instant application, such as:

United States Patent No. 7,251,326 B2 to Kurdziel, which is cited to show a similar device to the one claimed in the instant application.

43. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

44. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

45. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf